Sindh Univ. Res. Jour. (Sci. Ser.) Vol.50 (3D) 55-58 (2018)

SINDH UNIVERSITY RESEARCH JOURNAL (SCIENCE SERIES)

Cybercrime an emerging challenge for internet users: An overview

N. I. ALI, S. SAMSURI, M. S. A SEMAN, I. A. BROHI, A. SHAH

Department of Information Systems, International Islamic University Malaysia

Received 10th June 2018 and Revised 15th September 2018

Abstract: Any crime in which computer is target or tool used to conduct the crime is called cybercrime. The internet has gain more popularity in last two decades, world has become global village, on the one hand it is serving the humanity because it has make the life of people very easy, for example people can share and access the information, can do the online social transactions and buying, interact with each other at very low cost. On the other hand, it has become best place of crime for many cybercriminals. People are facing different types of cybercrimes like phishing, fraud, identity theft, Email Spoofing, bullying, cyber stalking, Malware, computer virus. In this paper author discussed the history of cybercrime, different types of cybercrime and their effect on internet users, the possible ways to protect our self for being a cybercrime victim.

Keywords: Internet, Cybercrimes, Cybercriminals, Types of cybercrimes, History.

1. INTRODUCTION

Internet users are growing rapidly since the last four decades. Nearly four billion peoples around the globe are online, that shows that half of the world using the internet nowadays, out of which half of the individuals started using it since 2017 ("internet world Stats," 2018). World statistics show the dramatic increase in the users of the internet. **(Fig. 1)** shows the penetration of internet users around the globe. Whilst, statistics revealed that 95% Americans are using the internet in their routine activities, whereas, in total 49% of the population using the internet in Asia, the number of internet users increased rapidly from 2017 to 2018 ("internet world Stats," 2018).

WORLD INTERNET USAGE AND POPULATION STATISTICS
DEC 31, 2017 - Update

World Regions	Population (2018 Est.)	Population % of World	Internet Users 31 Dec 2017	Penetration Rate (% Pop.)	Growth 2000-2018	Internet Users %
Africa	1,287,914,329	16.9 %	412,150,114	32.0 %	9,029.7%	10.2 %
Asia	4,207,588,157	55.1 %	1,992,360,400	47.4 %	1,643.0%	49.2 %
Europe	827,650,849	10.8 %	700,150,752	84.6 %	566.2%	17.3 %
Latin America / Caribbean	652,047,996	8.5 %	424,628,388	65.1 %	2,250.0%	10.5 %
Middle East	254,438,981	3.3 %	147,117,259	57.8 %	4,378.7%	3.6 %
North America	363,844,662	4.8 %	345,660,314	95.0 %	219.8%	8.5 %
Oceania / Australia	41,272,958	0.6 %	28,180,356	68.3 %	269.8%	0.7 %
WORLD TOTAL	7,634,757,932	100.0 %	4,050,247,583	51.8 %	996.1%	100.0 %

NOTES: (1) Internet Usage and World Population Statistics estimates in Dec 31, 2017. (2) CLICK on each world region name for detailed regional usage information. (3) Demographic (Population) numbers are based on data from the United Nations Population Division. (4) Internet usage information comes from data published by Nielsen Online, by the International Telecommunications Union, by GfK, by local ICT Regulators and other reliable sources. (5) For definitions, navigation help and disclaimers, please refer to the Website Surfing Guide. (6) The information from this website may be cited, giving the due credit and placing a link back to www.internetworldstats.com. Copyright © 2018, Miniwatts Marketing Group. All rights reserved worldwide.

Fig. 1. Internet users around the globe… Source ("internet world Stats," 2018)

As the popularity of the internet is increasing day by day, along with providing many benefits such as ease of use, time-saving, and convenience, it also invites the criminals to perform the cybercrimes very easily. Crime means something illegally done. Cybercrime refers to execution of unlawful activity by using cyberspace as the source of crime. Cyber security refers to "a measure for protecting computer systems, networks, and information from disruption or unauthorized access, use, disclosure, modification or destruction" (Gallaher, Link and Rowe, 2008). In the recent years, the world has witnessed the swift rise in the cybercrimes due to the increase in use of internet. Internet has connected the computers of world, it has became easier for cybercriminals to conduct the cybercrime. Unlike the physical crimes, the virtual crimes can be done remotely without geographical boundaries and sometimes it becomes very hard to trace them and collect the digital evidence (Hui, and Wang, 2017).

2. BACKGROUND

The existence of cybercrime can be traced before the presence of Microsoft, personal computer, internet and windows (Thomas.2008). First Cybercrime was conducted in 1820 in a fabric company of France, when the Joseph-Marie Jacquard produce the looms for repetitive use in weaving the clothes. This caused insecurities among other employees and they managed to stop him from further use of the new technology and modifying the loom patterns (Dalla and Geeta, 2013; Mohiuddin, 2006; Nagpal, 2008; Rajput, n.d.). The traces of cyber crime is available since 1960's when the internet was not yet invented but the cybercriminals were already existed inside the organization, who were harmful to their organizations (Dineshbhai and Patel, 2017). First, officially registered cybercrime was conducted in 1964 by the young student of Massachusetts Institute of Technology (MIT), the pattern of crime was to unofficially access the long-

++ Corresponding author: Najma Imtiaz Ali email: najma.channa@usindh.edu.pk
*Institute of Mathematics & Computer Science University of Sindh, Jamshoro,

distance calls by inhabiting the ringing tone (Thomas, 2008). In 1986 another more serious cybercrime was reported where the systems administrator at the 'Lawrence Berkeley National Laboratory', Clifford Stoll, noted certain irregularities in accounting data, where the cybercriminals stolen the army data and passed it to enemies, Stoll takes the measure and the criminals were arrested and send to prison (Tech, n.d.). After that, many cybercrimes were reported around the world. The one of the major cybercrime reported in 2012 at the South Carolina Department of Revenue', when cyber criminals broke the system and steal 3.6 million Security numbers and 387,000 credit/debit card numbers (Dineshbhai and Patel, 2017).

2.1 Classification of Cybercrimes.

Carter David divides the cybercrime in four broad categories. (David. 1995)

a) **Computer as the Target**: The crime in which computer is target to steal the personal information related to individuals or marketing companies and that steal data can be used for blackmailing purpose.

b) **Computer as the Instrumentality of the Crime**: The category of cybercrimes in which computer or its processes used to conduct the crime but not directly the data that is available to computer.

c) **Computer Is Incidental to Other Crimes**: In this category computer is not essential device to conduct the crime but its related technologies can be use to faster the crime process and also make it difficult to analyse the crime laundering and unlawful ban transactions are its example.

d) **Crimes Associated with the Prevalence of Computers:** The crimes which are the result of innovations of computer technology, especially with the introduction of microcomputers, which can be one of the reasons for dispersion of more cybercrime activities.

Cybercrime can be classified in two types

1. Crimes that directly target the computer networks or devices, for example hacking, malware, computer virus, Daniel-of-Service (DoS).

- **Hacking-** it is attempt by the cybercriminals also called hackers in this case to access your computer without permission. Some hackers do this just to get the popularity whereas others do this to give harm to their enemies and other institutions. 'Black Hats' and Crackers are also the Hackers. Hackers are usually the high-level programmer. Some companies hire the Hackers called 'White Hackers' to investigate their system flaws and fix them before the attack of the Hacker's
- **Malware-** This is the short form of malicious software. The malware is a virus, which attach itself with computer program and can circulate over the network. Malware, virus or worm can be used interchangeably. The malware is capable of occupying and destroying the computer memory and can be a cause of loss.
- **Daniel-Of-Service(DOS)-** It is an attempt by criminals to deny the service requested by the users. The cybercriminals send the unlimited requests to the server, which cause the overloading of the server and the user cannot receive their required services from the server. DOS usually attacks the high-profile websites, including institution.

2. Crimes that uses computer or internet to conduct the crime, for example Fraud, identity theft, cyberstalking, Phishing, Email spoofing, Password sniffing

- **Fraud-** Often called credit card fraud can happened by using your credit card details. Do not forget to receive your receipt after by the credit card. Be careful when doing online buying. Never save your credit card number with the online website. This type of crime usually happened when you drop your pre-pin debit/ credit card, the criminals take the opportunity to shop until the card is blocked.
- **Identity theft-** when someone else theft your identity and pretend as you is called identity theft. The cybercriminals used the identity of the victim to access their accounts, and other activities. Many time the cybercriminals use the lost documents or inbox to take the loan.
- **Cyberstalking-** Cyberstalking can be done through cyber stalker by virtually follow their victim through the internet. They cannot harm their victims physically but can give them mentally torture. Cyberstalker, usually keep an eye on the internet activities of victim and can blackmail him/ her. Victim for cyberstalking are usually women and the kids who are not familiar with the security measures of internet usage.
- **Phishing-** It means to extract the confidential data such as debit/credit card information. Accounts username and password combination. This can be done through e-mail spoofing and password sniffing. The phisher sends the victim the spoof emails pretend to be from their institutions. If the victim access that email than phisher malware software can attack your system and get the sensitive data i.e. password of accounts, which can be used to access your data.

2.2 Who can be cybercriminals?

The cybercriminal are divided into three categories.

a) Cybercriminals who done the cybercrimes only to seek the recognition, this types of criminals are usually youngster and want to be famous that's why conduct the cybercrimes.(Bhat and Khan, 2015)

b) Cybercriminals, who wants to make quick. They are usually involved in the online crimes, transactions and

frauds. Their main aim is to commit fraud and transfer amount of the victims into their accounts (Bhat and Khan, 2015)

c) Third and most dangerous category is the one who commit cybercrimes, just to harm the state or any country, their main aim is to just fight a cause so they did not care to whom they are giving the destruction. They are called cyber-terrorist (Bhat and Khan, 2015)

3. MATERIALS AND METHODS

In this section, we discuss the concepts, tools and methods utilized in the preparation of this paper.

3.1 Recent report on cybercrime by Internet Crime Complaint Centre (IC3)

The (IC3) was established by USA in 2000, the main purpose of this organization is to receive and investigate cyber crime cases around the world. There have been 4,063,933 crimes reported. According to report released by IC3 in 2017 approximately 284,000 complaints are reported each year. The loss of $1.42 billion by victims was reported in 2017 (IC3, 2017) as shown by **(Fig. 2)**.

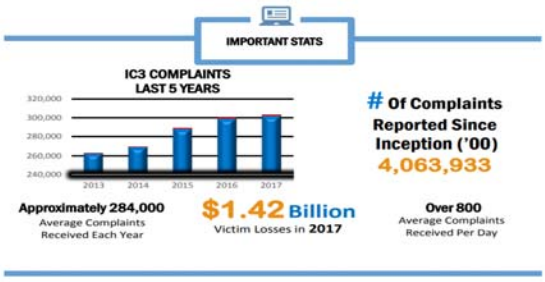

Fig 2. Cybercrime complaints from all over the world to IC3 (IC3, 2017)

(Table 1) shows the age wise victims and loss reported during 2017, there were total loss of $1,095,255,921 in 2017 (IC3, 2017). We can notice from table 1, as the age increases, the number of victims and volume of loss also increased.

Table 1. Number of victims and loss in2017 IC3 report (IC3, 2017)

VICTIMS		
Age Range	Total Count	Total Loss
Under 20	9,053	$8,271,311
20 - 29	41,132	$67,981,630
30 - 39	45,458	$156,287,698
40 - 49	44,878	$244,561,364
50 - 59	43,764	$275,621,946
Over 60	49,523	$342,531,972
Total	**233,808**	**$1,095,255,921**

IC3 is very active in generating reports every year regarding to the cyber-attacks around the globe. It provides detailed and complete information in order to increase awareness among people regarding types of crimes, total losses and other related information. IC3 is preparing the reports related to cybercrime every year and with the collaboration of FBI. Similarly these reports are distributed across the world, whereas, other developed countries such as United Kingdom and Canada are also trying to establish similar type of centres (Abubakar, *et al.,* 2015).

Table 2.Top 20 foreign countries (IC3, 2017)

TOP 20 FOREIGN COUNTRIES 2017							
1. Canada	3,164	6.Russian Federation	594	11. France	368	16. Netherlands	266
2. India	2,819	7. Brazil	558	12. China	366	17. Malaysia	265
3.United Kingdom	1,383	8. Germany	466	13.South Africa	349	18.United Arab Emirates	259
4. Australia	989	9. Philippines	453	14. Italy	291	19. Spain	248
5. Mexico	632	10. Japan	413	15. Pakistan	276	20. Argentina	238

(Table 2) shows the top 20 countries by victims who reported to IC3 except America for which separate table was given with state wise reported numbers. Most cases were registered in California State, with 41,974 victims. Table 2 demonstrates that highest cases in 2017 were registered from Canada i.e. 3,164 whereas lowest cases were registered from Afghanistan i.e. 238 (IC3, 2017). With the efficient measures taken by the government of each country, these crimes can be reduced. Every country should impose the cyber law in order to prevent their people being the victim of cybercrime. **(Fig. 3)** shows the types of cybercrime with victims count in 2017. Most crimes happen under the category of Non-payment/ Non-Delivery with 84079 victims whereas least cases reported under the Hacktivist category with 158 victims. (IC3, 2017)

2017 Crime Types

By Victim Count			
Crime Type	Victims	Crime Type	Victims
Non-Payment/Non-Delivery	84,079	Misrepresentation	5,437
Personal Data Breach	30,904	Corporate Data Breach	3,785
Phishing/Vishing/Smishing/Pharming	25,344	Investment	3,089
Overpayment	23,135	Malware/Scareware/Virus	3,089
No Lead Value	20,241	Lottery/Sweepstakes	3,012
Identity Theft	17,636	IPR/Copyright and Counterfeit	2,644
Advanced Fee	16,368	Ransomware	1,783
Harassment/Threats of Violence	16,194	Crimes Against Children	1,300
Employment	15,784	Denial of Service/TDoS	1,201
BEC/EAC	15,690	Civil Matter	1,057
Confidence Fraud/Romance	15,372	Re-shipping	1,025
Credit Card Fraud	15,220	Charity	436
Extortion	14,938	Health Care Related	406
Other	14,023	Gambling	203
Tech Support	10,949	Terrorism	177
Real Estate/Rental	9,645	Hacktivist	158
Government Impersonation	9,149		

Fig 3. Cybercrime complaints from all over the world to IC3 (IC3, 2017)

4. DISCUSSION

As the internet connects the computer of all over the world together, it also invites the criminal minds' to access and attack the once privacy without the geographical boundary. Cybercrime has become on of the emerging challenges for the internet users around the globe. As the number of internet users have increased, it also provides the cybercriminals to access their activities. The cybercriminals can attack the individuals or organizations to fulfil their dirty needs. The internet users must take measures to keep safe their selves from cybercriminal attacks.

- Keep data secure like your username and password. Do not share this information with anyone.
- Always use the strong password.
- Always deals with the trusted websites for online (Ali, Samsuri, Sadry, Brohi, & Shah, 2016)
- Always install the strong antivirus on your smart devices and computer.
- Do not open the unknown emails.
- Do not response to any email, which is asking for username and password of your accounts, because these institutes never request this type of information online.
- Most importantly, if anyone face cybercrime activity, he or she should report it.

5. CONCLUSION

In this paper, authors discussed the challenges faced by the internet users in the form of cybercrimes. It was observed that the cybercrime was there before the invention of internet. Different types of cybercrimes and cybercriminals also discussed in this paper. The recent report issued by the IC3, one of the largest organization to report and solve the cybercrimes around the globe was also discussed. In last the possible prevention from the cybercrimes were discussed.

REFERENCES:

Abubakar, A. I., H. Chiroma, S. A. Muaz, and, L. B. Ila (2015). A review of the advances in cyber security benchmark datasets for evaluating data-driven based intrusion detection systems. Procedia Computer Science, 62(Scse), 221–227. http://doi.org/10.1016/j.procs.2015.08.443

Ali, N. I., S. Samsuri, M. Sadry, I. A. Brohi, and A. Shah, (2016). Online Satisfaction in Malaysia: A Framework for Security, Trust and Cybercrime. In *2016 6th International Conference on Information and Communication Technology for The Muslim World (ICT4M)* (pp. 194–198). IEEE. http://doi.org/10.1109/ICT4M.2016.048

Bhat, T. H., A. A. Khan, (2015). Cybercrimes , security and challenges, *4*(5), 509–513. http://doi.org/10.17148/IJARCCE.2015.45108

Dineshbhai, V., M. Patel, (2017). Growing Cybercrimes in India: A Survey. Retrieved from http://www.ijirst.org/articles/SALLTNCSP003.pdf

Dalla, S. H. E., M. Geeta, (2013). Cyber Crime – A Threat to Persons, Property, Government and Societies. Ijarcsse, 3(5), 997–1002.

David.L.Carter. (1995). computr crime categories.

Hui, K. L., S. H. Kim, Q. H. Wang, (2017). Cybercrime Deterrence and International Legislation: Evidence from Distributed Denial of Service Attacks. *MIS Quarterly*, *41*(2), 497–523. http://doi.org/10.25300/MISQ/2017/41.2.08

IC3. (2017). Internet Crime Report. Retrieved from https://pdf.ic3.gov/2017_IC3Report.pdf

Internet world Stats. (2018). Retrieved from https://www.internetworldstats.com/stats.htm

Michael P., G. Albert N. Link, Brent R. Rowe. (2008). Cyber Security. Cheltenham: Edward Elgar Publishing Limited.

Mohiuddin, Z. (2006). a Paper Presented on : Cyber Laws in Pakistan ; a Situational Analysis and.

Nagpal, R. (2008). Evolution of Cyber Crimes. Rohas Nagpal.

Rajput, A. (n.d.). Cyber Crime. Academia. Retrieved from http://www.academia.edu/1869461/Cyber_Crime

Tech, F. (n.d.). A Brief History of Cyber Crime. Retrieved August 11, 2018, from https://www.floridatechonline.com/blog/information-technology/a-brief-history-of-cyber-crime/

Thomas, C. and N. Balakrishnan, (2008). Performance enhancement of Intrusion Detection Systems using advances in sensor fusion. 2008 11th International Conference on Information Fusion, 1–7